Załącznik numer 2
do Polityki bezpieczeństwa
przetwarzania danych osobowych
w PROTEKTOR Sebastian Piórkowski

INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA ZASAD OCHRONY DANYCH OSOBOWYCH.

§1
Postanowienia ogólne

1. Instrukcja niniejsza określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku, gdy:
   1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
   2) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, mogą wskazywać na naruszenie zabezpieczeń danych.
2. Osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie, jest Administrator Danych Osobowych.

§2
Sytuacje naruszenia ochrony danych osobowych

1. Za naruszenie ochrony systemu informatycznego uważa się w szczególności:
   1) naruszenie lub próbę naruszenia integralności systemu oraz zbioru danych,
   2) nieuprawniony dostęp lub próbę dostępu do systemu lub pomieszczeń (widoczne uszkodzenia bądź naruszenia zabezpieczeń),
   3) nieautoryzowane zniszczenie lub próbę zniszczenia danych zgromadzonych w systemie,
   4) zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany,
   5) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   6) inny stan systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem,
2. Instrukcję stosuje się odpowiednio w przypadku stwierdzenia, że stan pomieszczeń i szaf, bądź innych mebli biurowych, w których przechowywana jest dokumentacja lub zawartości tej dokumentacji wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby trzecie.

§3
Przedsięwzięcia organizacyjne zabezpieczające przed naruszeniem systemu ochrony danych osobowych

1. Do pomieszczeń, gdzie przetwarza się dane osobowe winny mieć stały dostęp tylko osoby upoważnione przez Pracodawcę
2. Klucze do pomieszczeń gdzie przetwarza się dane osobowe winny być przechowywane po godzinach pracy przez ochronę budynku, a sposób ich wydawania i ochrony określają odrębne uregulowania.
3. Klucze zapasowe do pomieszczeń, w zapieczętowanej kopercie winny być przechowywane w specjalnej szafie.
4. Dokonuje się stałych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń i ochrony w danym wydziale.

§4

Postępowanie w przypadku stwierdzenia lub podejrzenia zaistnienia naruszeń zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe.

1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie zabezpieczeń systemu informatycznego, w którym przetwarzane są dane osobowe, użytkownik systemu zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Danych Osobowych
2. Użytkownik niezwłocznie:
   1) zabezpiecza dostęp do miejsca lub urządzenia przez osoby trzecie,
   2) wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane,
   3) podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
3. Administrator Danych Osobowych po przybyciu na miejsce, w którym doszło do naruszenia ochrony danych osobowych:
   1) ocenia zastaną sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane, stan urządzeń i zbioru danych oraz identyfikuje wielkość negatywnych następstw naruszenia ochrony danych osobowych,
   2) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, odłączenie wadliwych urządzeń, zmiana haseł, blokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych),
   3) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia, jak również sprawdza zawartość zbioru danych osobowych,
   4) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   5) sprawdza sposób działania programu (w tym również obecność wirusów komputerowych),
   6) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,
   7) niezwłocznie zapewnia przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia baz danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,
   8) sprawdza jakość komunikacji w sieci telekomunikacyjnej,
   9) dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,

4. Zgodę na uruchomienie komputerów i innych urządzeń oraz kontynuowanie pracy wyraża Administrator Danych Osobowych zarządzający sieciami i systemami informatycznymi.
5. Dokonywanie zmian w miejscu naruszenia ochrony bez uzyskania zgody, o której mowa w ust. 4 jest dopuszczalne, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.
6. Administrator Danych Osobowych podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:
   1) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,
   2) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje o wyciągniecie konsekwencji służbowych lub innych przewidzianych przepisami.